УДК 004.056.53

Бакін Д.С.
Кіровоградський національний технічний університет

Проблеми захисту інформації в комп`ютерних мережах

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку внутрішніх порушників , так і зовнішніх.

Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних. При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти початкову продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Основні проблеми, що виникають з безпекою передачі інформації в комп'ютерних мережах, можна поділити на такі :

— Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

— Модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

— Підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від чужого імені (цей вид обману прийнято називати спуфінгом) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Потреби сучасної практичної інформатики призвели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є автентифікація електронної інформації в умовах, коли сторони що обмінюються інформацією не довіряють одна одній. Ця проблема

пов'язана зі створенням систем електронного цифрового підпису. Технічною основою переходу в інформаційне суспільство є сучасні мікроелектронні технології, які забезпечують безперервне зростання якості засобів обчислювальної техніки і служать базою для збереження основних тенденцій її розвитку - мініатюризації, зниження електроспоживання, збільшення обсягу оперативної пам'яті (ОП) і місткості вбудованих і змінних накопичувачів, зростання продуктивності і надійності, розширення сфер і масштабів застосування. Дані тенденції розвитку засобів обчислювальної техніки призвели до того, що на сучасному етапі захист комп'ютерних систем від несанкціонованого доступу характеризується зростанням ролі програмних та криптографічних механізмів захисту в порівнянні з апаратними.

Зростання ролі програмних і криптографічних засобів захисту проявляється в тому, що виникають нові проблеми в галузі захисту обчислювальних систем від несанкціонованого доступу, вимагають використання механізмів і протоколів з порівняно високою обчислювальною складністю і можуть бути ефективно вирішені шляхом використання ресурсів ЕОМ.

Виникнення глобальних інформаційних мереж типу INTERNET є важливим досягненням комп'ютерних технологій, однак, з INTERNET пов'язана маса комп'ютерних злочинів.

Результатом досвіду застосування мережі INTERNET є слабкість традиційних механізмів захисту інформації та відставання у застосуванні сучасних методів.

Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи з впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Інформація повинна бути захищена в першу чергу там, де вона створюється, збирається, переробляється і тими організаціями, які несуть шкоди безпосередній при несанкціонованому доступі до даних. Цей принцип є як раціональний так і ефективний: захист інтересів окремих організацій – це складова реалізації захисту інтересів держави в цілому.

Список використаних джерел

1. *Означення поняття криптографя[Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Криптограія.*
2. *Про проблеи захисту інформації в комп`ютерних мережах [Електронний ресурс]. – Режим доступу: http://ua-referat.com/.*
3. *Про завдання захисту електронної інформації [Електронний ресурс]. – Режим доступу: http://ua.textreferat.com/.*